IPv6 in Access Networks: Challenges and Opportunities

Tim Stevens, Koert Vlaeminck, Wim Van de Meerssche, Filip De Turck, Bart Dhoedt, Piet Demeester
UGent – IBBT – IMEC
Gaston Crommenlaan 8, B-9050 Gent, Belgium
Tim.stevens@intec.ugent.be, Tel: +32 (0)9 331 49 39

Enrique Areizaga Sanchez
ROBOTIKER TELECOM, TECNALIA
Parque Tecnológico, Edificio 202. E-48170 Zamudio (Bizkaia) (SPAIN)
enrique@robotiker.es, Tel: +34 94 600 22 66

Abstract

IPv6's 128-bit addressing space, providing public addresses for each connected device, is the single most important improvement of IPv6 over IPv4. This paper illustrates how regaining end-to-end connectivity can enable multi-service delivery in a converged access network. Of course, migration to IPv4's successor introduces interesting technical challenges, especially from a security perspective.

1 Introduction

Designing a next-generation access network, IPv4's successor cannot be overlooked. IPv6 [1] provides a virtually unlimited addressing space, stateless and stateful host autoconfiguration mechanisms, extended QoS (Quality of Service) support in the IP header and improved mobility support, to name just a few advantages.

If the Muse [2] architecture has to become an extensible platform, enabling a seamless and effortless deployment of new services, IP end-to-end connectivity is highly desirable. Network Address Translation (NAT) [3] – IPv4's answer to the shortage of IP addresses – requires all network connections to be instantiated by the client device behind the NAT gateway, thereby seriously limiting the connection setup possibilities and hence, the types of services that could be offered by the multi-service access network. IPv6 re-introduces IP end-to-end connectivity by providing 128-bit addresses (cf. Figure 1). Additionally, given the increasing number of mobile devices, support for a service-aware nomadic environment would be highly desirable. Again, this is not possible when IP end-to-end connectivity is broken: individual terminals/users behind a NAT gateway cannot be distinguished, a priori disabling end-to-end service profiles.

Of course, the new network protocol should be considered merely as an enabler, necessary for a service aware environment. New and enhanced fields in the IPv6 header (e.g. QoS related fields) and new features (e.g. IPsec) only act as a placeholder and filling them in with useful values and mechanisms is the major challenge for the novel access platform. Moreover, the absence of NAT's implicit security advantage necessitates the introduction of a security management system that defines policy enforcement points in the access network.

2 IPv6 Opportunities in Access

Until recently, the majority of Internet applications were based on a client-server communication principle. Examples of these applications are web browsing, e-mail, FTP or Telnet/SSH. Except for FTP data connections, all sessions and requests are initiated on the client side. This behavior is especially important for NAT solutions, where the NAT gateway sets up a connection to the server on behalf of the client, thereby manipulating the private source IP address and TCP/UDP source port. Data sent back from the server to the client is again mapped to the private address in the NAT gateway. This principle works well for client-initiated sessions, but prevents session initiation by a remote host outside the private network. Novel Internet applications are mostly communication-oriented (e.g. VoIP) and obsolete the client-server communication paradigm. As depicted in Figure 1, direct communication between peers is impossible using IPv4. By consequence, development and deployment of new services is hampered and existing peer-to-peer applications are adapted to be mediated by a server with a public IP address. This limits scalability and generates unnecessary overhead, while being contrary to the general IP philosophy. By re-introducing end-to-end connectivity, IPv6 opens the door for new Internet applications.

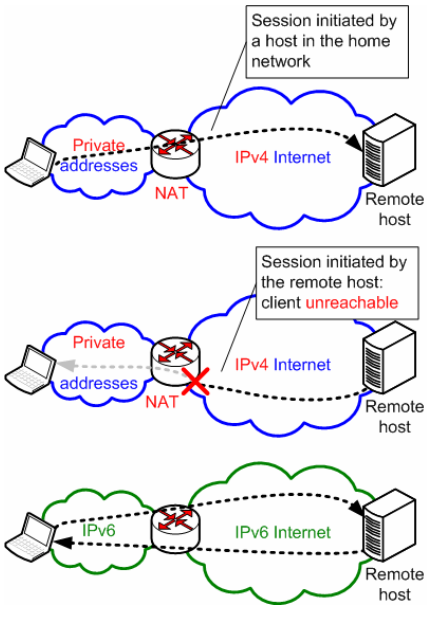

Figure 1: IPv6 end-to-end connectivity

Evolving to an all-IP converged access network, end-to-end connectivity has the additional advantage of allowing per-device subscriber identification. Based on the subscriber and device identification data, end-to-end connection or service profiles can be enabled (cf. Figure 2). Combining a multi-service access environment – with service-specific network requirements – and the growing popularity of mobile devices, this property might become significant.

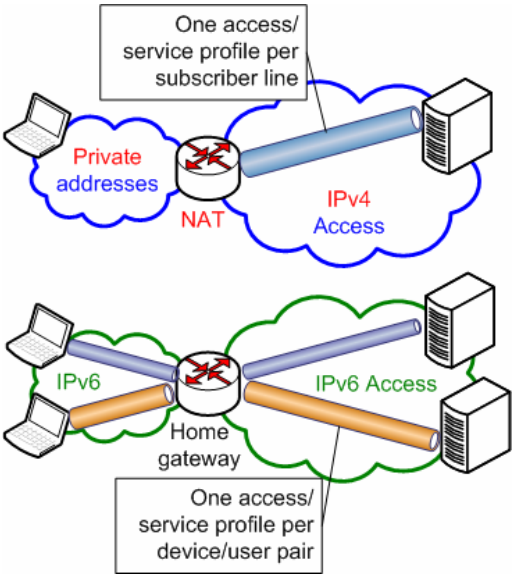

Figure 2: Per user/device service profiles

Furthermore, network-layer security – an optional feature using IPv4 – can only be applied when end-to-end transparency is available. The IPv6 standard dictates IPsec implementation, thereby enabling the possibility for network-layer secure communication between two arbitrary hosts in the network.

3 Access network architecture challenges

While re-introducing end-to-end connectivity clearly opens the door for deploying new services, it cannot be denied that IPv4's NAT solution provides implicit security features, by disallowing connections setup outside the private network to pass the NAT gateway. As depicted in Figure 3, access network IP aggregation points and subscriber gateways can be extended to provide security services to home networks. As opposed to the NAT approach, this would allow fine-grained per user/device security settings, without a priori disabling incoming connections for a device connected to the home network. Apart from security management, per user/device authentication in this connectionless environment definitely needs further investigation too. In this respect, the IETF PANA (Protocol for carrying Authentication for Network Access) charter [4] provides interesting draft documents, including a proposal for network authentication based on IPsec.

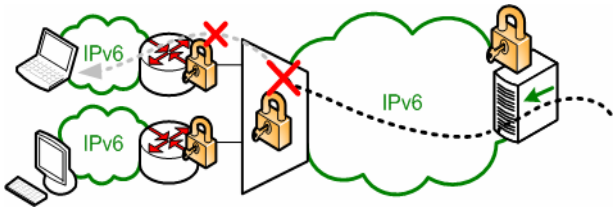

Figure 3: Security in IPv6 access networks

As mentioned in the previous section, IPv6 access networks could allow for per user/device access and/or service profiles. In addition to allowing or disallowing access to specific services offered by the access-, network- or application provider, QoS parameters could be assigned to specific access- and/or service profiles. Taking into account the convergence of existing communication networks into a single IP solution carrying different types of data, QoS support becomes increasingly important. While IPv6 provides substantial QoS features in its IP header, designing a QoS management system that supports per-service/per-user differentiation throughout the access network is not a trivial task.

Conclusions

As illustrated in this paper, IPv6 can act as a true enabler for a service aware access environment by regaining IP end-to-end connectivity. The usage of additional IPv6 features (e.g. QoS, IPsec) presents interesting opportunities and challenges for both application-layer and access network architecture research and development. Moreover, the absence of NAT's implicit security advantage necessitates the introduction of a security management system that defines policy enforcement points in the access network.

Apart from the above-mentioned technical advantages, it should be taken into account that providing IPv6 support in next-generation European access networks can result in a substantial strategic advantage, by anticipating the massive deployment of IPv6 networks in Asia.

Acknowledgments

This work is supported by the IST FP6 MUSE project. MUSE contributes to the strategic objective "Broadband for All" of IST (Information Society Technologies) and it is partially funded by the European Commission.

References

1. S. Deering and R. Hinden, "RFC 2460: Internet Protocol, Version 6 (IPv6) Specification," IETF, 1998
2. Multi Service Access Everywhere. [Online]. Available: http://www.ist-muse.org/
3. G. Tsirtsis and P. Srisuresh, "RFC 2766: Network Address Translation - Protocol Translation (NAT-PT)," IETF, 2000
4. Protocol for carrying Authentication for Network Access. [Online]. Available: http://www.ietf.org/html.charters/pana-charter.html